4. Reported by:

INCIDENT INFORMATION

5. Date:	6. Time:
7. Location (site, building, room):	
8. Equipment/system involved:	
8a. Sensitivity/criticality level (Check One): ☐ Level 1 ☐ Level 2	
8b. Classified information involved: ☐ Yes ☐ No	
9. Data or system owner:	
10. DPI/CSO:	
11. Description (continue on separate sheet if necessary):	

INFORMATION TECHNOLOGY SECURITY (ITS) INCIDENT PROCEDURE
For assistance, call the Center ITS Manager (C-ITSM) at (256) 544-1223

1. ITS incidents (such as theft, vandalism, significant misuse, privilege and access abuse, threats, and the intentional spread of malicious code, or suspicion based on evidence of such incidents) involving Government and contractor automated information resources must be reported. It is the responsibility of the Data Processing Installation Computer Security Official (DPI CSO) to ensure that the C-ITSM is kept informed. Cases involving theft, fraud, abuse, and vandalism should be reported immediately to the Manager of Protective Services Department (AD50).

2. To achieve our primary responsibility to save assets first, actions must be taken immediately to protect the affected systems and keep the problem from spreading. This form must be completed as quickly as the situation allows. It is very important that good notes and logs are kept of the symptoms or evidence.

3. If an incident is detected or suspected by discovery through hardware or software maintenance, virus eradication, or user notification, the C-ITSM will be notified. Notification requires documenting the incident through the use of this form. Emergency situations should be reported immediately by telephone to the C-ITSM.

4. Significant ITS incidents involving Government employees will be reported by the C-ITSM to the Human Resources Department (CD10) for appropriate action. Significant incidents involving contractor employees will be reported to the Contracting Officer's Technical Representative by the C-ITSM for appropriate action.

5. A follow-up review must occur to assure that appropriate corrective measures have been taken. The incident must be addressed in the first DPI risk assessment and management plan occurring following the incident, including validation that corrective measures have been taken to minimize future occurrences.